Sorenson Communications®

CaptionCall®

IMPORTANT SECURITY ALERT AND URGENT ACTION ITEMS FROM SORENSON COMMUNICATIONS

March 21, 2014

To all United States Sorenson Communications and CaptionCall® employees:

An email was sent to all employees on March 11 regarding unauthorized access to Sorenson employee data. This letter is being sent to you as a follow-up communication. If you did not receive or were unable to read that email, it is very important for you to know that the personal information stored in your Sorenson Human Resources (HR) account was subject to unauthorized access. This means that you and those listed in your Sorenson HR account may be at risk of identity theft and fraud. You should take action immediately.

On March 7, 2014, we determined that between February 20 and March 3, 2014, Sorenson's account with the vendor that handles payroll for Sorenson Communications and CaptionCall® employees was subject to several malicious attacks. Those attacks successfully accessed personal information that employees provided as part of their HR data. The personal information accessed affects you as well as your beneficiaries, dependents, and emergency contacts—those listed in your Sorenson HR account. Accessed information included name, date of birth, address, Sorenson income history, Social Security Numbers, W-2 information, and emergency contact data.

Sorenson is investigating this incident with the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS). While those investigations are ongoing, they have not required us to delay notifying you of this incident. Since learning of the data theft, Sorenson has implemented additional levels of security. We are taking every step necessary to address employee concerns and to provide employees and all those affected with credit and identity theft protection through Experian Corporation, one of the three major U.S. credit reporting and protection companies.

At this time, Sorenson has no evidence that employees' banking information was exposed. However, you may want to inform your bank and other financial institutions that your personal information has been compromised.

It is important that you remain vigilant about protecting yourself and those listed in your Sorenson HR account from identity theft and fraud. There are a number of steps you should take, including informing the credit reporting agencies that your information has been compromised and diligently monitoring your bank accounts and credit reports for indications of fraud. If you have not done so already, **please follow the instructions in the March 11 email** to enroll in the company-provided credit monitoring and to take other protective measures. If you have dependents or others listed in your Sorenson HR account, you were also sent an email on March 14. **Please complete the instructions in both email(s) as soon as possible!** While this takes time and is inconvenient, it is very important that you protect yourself and those you may have listed in your Sorenson HR account. ***If you did not receive email from Sorenson on March 11, you should immediately contact Human Resources Support at*** hrsupport@sorenson.com to obtain activation codes and instructions for credit monitoring and identity theft insurance provided by the company at no cost to you. The enclosed information does not replace the information in the emails, but provides a review of it.

To verify who is listed in your HR account, and the information stored for each contact, visit UltiPro at https://n11.ultipro.com, log in, click on "Myself," and select "Contacts" from the menu.

Sorenson sincerely regrets and apologizes to you and to your families for this unfortunate situation. If you have additional questions about this information or the instructions included in the emails, please email hrsupport@sorenson.com.

Sincerely,

Joe Tate
Vice President, Human Resources
Sorenson Communications

ADDITIONAL INFORMATION

Please retain this important letter – you may want to refer to it again.

Because your personal information has been compromised, you should:

1.) Enroll in Experian's ProtectMyID Alert service. Sorenson Communications is providing a prepaid, one-year membership to this service for each employee and those listed in Sorenson HR accounts. If you have not done so already, it is important that you take advantage of this offer right away. Experian's ProtectMyID Alert service helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. The toll-free number for questions about enrollment is 877-371-7902. The enrollment deadline is June 30, 2014. *If you have not received emails with instructions and activation codes, you should contact Sorenson Human Resources at hrsupport@sorenson.com as soon as possible.*

You can obtain additional information about fraud alerts and security credit freezes by contacting the following U.S. credit reporting agencies:

Equifax	**Experian**	**TransUnion**
PO Box 740256	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
800-525-6285	888-397-3742	800-680-7289

2.) Place a security freeze on credit files. State laws also provide immediate protection though a security freeze placed on credit files. Security freezes are only available to those who have credit files. To learn more, visit https://www.experian.com/freeze/center.html. Note: There may be a small charge for placing a freeze on credit files – this varies by state. After submitting an expense report, Sorenson will reimburse you for the security freeze costs for those associated with your Sorenson HR account. Sorenson is reimbursing only for the cost of security freezes. See the Experian website about the use and effects of setting and removing a security freeze.

3.) Call the IRS fraud reporting office at 800-908-4490 to report compromised tax information.

4.) After calling the IRS, fill out the individual IRS Form 14039. This form is available at http://www.irs.gov/Help-&-Resources/Tools-&-FAQs/FAQs-for-Individuals/Frequently-Asked-Tax-Questions-&-Answers/IRS-Procedures/Reporting-Fraud/Reporting-Fraud.

5.) You may also consider contacting your state Attorney General; contact information is available at: http://www.naag.org/current-attorneys-general.php.

If your personal information has been used fraudulently, you should:

1.) Use the Sorenson police report number 14-36713 if requested from law enforcement authorities. This will expedite your reporting process. Note that this case number was provided by the Unified Police Department of Salt Lake (Salt Lake County, UT U.S.A). You may obtain a copy of the full police report by requesting it from hrsupport@sorenson.com. You might also consider contacting your local police.

2.) Notify the Federal Trade Commission (FTC) that your information has been used fraudulently. The FTC identity theft hotline is 877-438-4338. Reference the police report number above. The FTC will also give you a reference number for your records. The FTC provides information about identity theft online at www.ftc.gov/idtheft. The FTC's address is:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

3.) Determine what other precautionary measures might be appropriate for your circumstances.

- **Consider obtaining an IRS Electronic Filing PIN**, if you do not already have one. Visit http://www.irs.gov/Individuals/Electronic-Filing-PIN-Request or call 866-704-7388 and follow the system prompts.

- **Manage personal information.**
  Take precautionary steps to protect personal information, such as carrying only essential documents. Be aware when sharing personal information. Shred receipts, statements, and other sensitive information when no longer needed.

- **Use tools from credit providers.**
  Carefully review credit reports, bank, credit card, and other account statements at least quarterly. Proactively create alerts on credit card and bank accounts for suspicious activity. If unauthorized or suspicious activity is discovered, do not delay! Take action immediately.

- **For general information regarding protecting personal information, visit**
  http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html.